

Załącznik nr 1 do Zapytania o wartość zamówienia

Zamówienie dofinansowane ze środków Unii Europejskiej, Krajowego Planu Odbudowy i Zwiększania Odporności finansowanego ze środków Instrumentu na Rzecz Odbudowy i Zwiększania Odporności; Inwestycja: C3.1.1.

Cyberbezpieczeństwo - CyberPL , infrastruktura przetwarzania danych oraz optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo; Cyberbezpieczeństwo - Cyberbezpieczny Rząd – w ramach projektu pn. „Cyberbezpieczeństwo w PIP”, na podstawie porozumienia o powierzenie grantu o numerze KPOD.05.10- CR.01-001/24/0036/ KPOD.05.10-CR.01-001/25/2025.

OPIS PRZEDMIOTU ZAMÓWIENIA

1. Przedmiot Zamówienia:

- 1) Przedmiotem zamówienia jest usługa polegająca na przygotowaniu i udostępnieniu na platformie e-learningowej szkolenia z zakresu cyberbezpieczeństwa pt. „Podstawy bezpieczeństwa cyfrowego w pracy”, dla maksymalnie 2800 pracowników Państwowej Inspekcji Pracy.
- 2) Szkolenie ma na celu podniesienie poziomu świadomości pracowników Państwowej Inspekcji Pracy w zakresie podstawowych zagrożeń cybernetycznych oraz zasad bezpiecznego przetwarzania informacji i korzystania z systemów teleinformatycznych.
- 3) Minimalny zakres tematyczny szkolenia powinien uwzględniać następujące zagadnienia:
 - a) Zagrożenia socjotechniczne, w tym m.in.:
 - (1) ataki socjotechniczne (techniki manipulacji wykorzystywane przez cyberprzestępców);
 - (2) sposoby - w jaki sposób wyłudza się informacje?
 - (3) wykrywanie - jak rozpoznać, że jest się celem ataku socjotechnicznego?
 - (4) reakcja - jak prawidłowo reagować na ataki socjotechniczne?
 - (5) jak i skąd atakujący zbierają dane na twój temat?
 - (6) miejsca, w których zostawiamy swoje dane świadomie i nieświadomie;
 - (7) podniesienie świadomości w zakresie udostępniania informacji w sieci.

- b) Bezpieczeństwo haseł, w tym m.in.:
 - (1) polityka haseł - jakie hasło jest bezpieczne, jak nimi zarządzać?
 - (2) zagadnienie aktualnego oprogramowania i kopii zapasowych;
 - (3) bezpieczna praca z przeglądarką internetową.
- c) Bezpieczeństwo poczty e-mail i ochrona przed SCAM-em
- d) Obrona przed phishingiem, w tym m.in.:
 - (1) odpowiedzialność pracownika przed pracodawcą za ujawnienie informacji;
 - (2) nieautoryzowane użycie systemów komputerowych;
 - (3) najczęstsze rodzaje naruszeń.
- e) Bezpieczeństwo stron WWW i przeglądarek
- f) Ataki socjotechniczne z wykorzystaniem urządzeń, w tym:
 - (1) przegląd aktualnych ataków komputerowych wykorzystywanych przez przestępców
 - (2) ataki przez pocztę e-mail (fałszywe e-maile);
 - (3) ataki przez strony WWW (jak nie dać się zainfekować);
 - (4) ataki przez komunikatory;
 - (5) ataki przez telefon (fałszywe SMS-y, przekierowania rozmów, itp.);
 - (6) ataki APT, phishing, smishing, spearphishing, pharming, spoofing, spam, spim, scam;
 - (7) najczęstsze zaniedbania związane z wykorzystywaniem sprzętu komputerowego.
- g) Zagrożenia związane z urządzeniami mobilnymi.
- h) Zagrożenia związane z sieciami Wi-Fi.
- i) Spoofing i phishing telefoniczny.
- j) Dobre praktyki bezpieczeństwa.
- k) Praca zdalna i zagrożenia z tym związane, w tym m.in.:
 - (1) bezpieczne korzystanie z urządzeń mobilnych w podróży (telefony, tablety, laptopy);
 - (2) bezpieczeństwo twojego otoczenia;
 - (3) bezpieczeństwo telepracy na prywatnym komputerze;
 - (4) bezpieczny zdalny dostęp do firmowych zasobów (VPN).

Wykonawca opracuje i przedstawi do akceptacji Zamawiającego program szkolenia, uwzględniając wskazane przez Zamawiającego zagadnienia.

2. Warunki realizacji zamówienia:

- 1) Szkolenie będzie realizowane w formie e-learningu, uwzględniając następujące zasady:
 - a) Szkolenie musi być zrealizowane w całości w języku polskim, zgodnie z zasadami ortografii i gramatyki języka polskiego oraz być wolne od błędów interpunkcyjnych, stylistycznych oraz błędów formatowania. Najważniejsze pojęcia wraz z wyjaśnieniem ich znaczenia znajdą swoje odzwierciedlenie w słowniku. Dostęp do zasobów słownika będzie możliwy dla Uczestnika szkolenia na każdym etapie realizacji szkolenia e-learningowego.
 - b) Na każdym ekranie lub slajdzie szkoleniowym Wykonawca musi zamieścić odpowiednie logotypy oraz informację o współfinansowaniu z ww. projektu.
 - c) Szkolenie musi składać się z części:
 - (1) informacyjnej (teoretycznej), która powinna być zakończona podsumowaniem wiadomości przekazanych w trakcie szkolenia,
 - (2) ćwiczeniowej (ćwiczenia typu „selftest”),
 - (3) sprawdzającej, tj. szkolenie musi być zakończone testem końcowym, którego zaliczenie będzie skutkowało uzyskaniem zaświadczenia potwierdzającego nabycie kompetencji. Test końcowy składać się będzie z pytań jednokrotnego lub wielokrotnego wyboru. Za zaliczenie testu końcowego uznaje się uzyskanie co najmniej 60% poprawnych odpowiedzi. W przypadku niezaliczenia testu końcowego uczestnik ma możliwość ponownego przystąpienia do testu bez dodatkowych kosztów, w okresie dostępności szkolenia. Po każdym niezaliczonym podejściu uczestnik otrzyma informację zwrotną umożliwiającą uzupełnienie wiedzy przed kolejnym podejściem do testu.
 - d) Szkolenie musi rozpoczynać się graficznym wstępem (intro).
 - e) Szkolenie musi posiadać narrację audio realizowaną przez lektora lub wysokiej jakości rozwiązanie lektorskie zapewniające naturalność przekazu.
 - f) Podczas szkolenia musi być zapewniona możliwość włączenia i wyłączenia dźwięku w całym szkoleniu, w pojedynczych modułach lub na pojedynczych ekranach.

- g) Szkolenie musi być interaktywne (minimalna liczba ekranów wymagających interakcji użytkownika musi stanowić co najmniej 40% wszystkich ekranów).
- h) Szkolenie musi zawierać zestaw ćwiczeń interaktywnych, pozwalających na samodzielną ocenę postępów w nauce i umożliwiających uzyskanie pełnej informacji zwrotnej na temat stopnia opanowania przez uczestnika zagadnień będących przedmiotem ćwiczeń.
- i) Szkolenie musi zawierać elementy multimedialne obejmujące między innymi: nagrania audio, animacje, elementy interaktywne. Nagrania audio oznaczają głos lektora oraz dźwięki sygnalizujące sukces lub porażkę.
- j) Mechanizmy zastosowane w szkoleniu będą umożliwiały uczestnikowi szkolenia przerwanie nauki w dowolnym momencie i ponowne jej kontynuowanie od miejsca, w którym zakończył.
- k) Wykonawca zapewni kolorystyczną szatę graficzną dobraną w sposób zapewniający czytelność treści, właściwy kontrast elementów graficznych oraz estetykę adekwatną do charakteru i przeznaczenia materiałów, z uwzględnieniem zasad dostępności, w szczególności odpowiedniego kontrastu kolorów.
- l) Szkolenie musi być intuicyjne w obsłudze i logicznie podzielone na moduły. Szkolenie musi rozpoczynać się wprowadzeniem (wstępem) prezentującym cel szkolenia, jego zakres tematyczny oraz sposób realizacji. Treść szkolenia powinna być logicznie podzielona na moduły tematyczne, umożliwiające stopniową i samodzielną realizację materiału szkoleniowego. W ramach modułów wymaga się przeprowadzania automatycznych testów wiedzy użytkowników lub ćwiczeń typu „selftest”, umożliwiających bieżącą weryfikację stopnia opanowania materiału.
- m) Szkolenie musi spełniać wymogi, normy i zasady WCAG 2.1 lub nowsze, obowiązujące w czasie realizacji szkolenia, w szczególności umożliwienie osobom z niepełnosprawnościami co najmniej zmianę kontrastu, wielkości czcionki oraz obsługę kluczowych elementów za pomocą klawiatury.

- 2) W celu oceny efektywności szkolenia Wykonawca zapewni możliwość dokonania przez uczestników wstępnej samooceny poziomu wiedzy i kompetencji w zakresie cyberbezpieczeństwa przed rozpoczęciem szkolenia (ankieta wstępna). Samoocena będzie mieć charakter informacyjny, ma na celu zobrazować aktualny poziom wiedzy uczestnika przed szkoleniem i nie będzie warunkiem przystąpienia do szkolenia ani uzyskania zaświadczenia.
- 3) Wykonawca, w terminie 5 dni roboczych od daty podpisania umowy opracuje i przedstawi Zamawiającemu do akceptacji dokumentację szkoleniową:
 - (1) program szkolenia,
 - (2) wzór zaświadczenia ukończenia szkolenia,
 - (3) wzór protokołu szkolenia.
- 4) Zamawiający uprawniony jest do wniesienia zastrzeżeń do dokumentacji, wskazanej w pkt 2 ppkt 3), w terminie 5 dni roboczych od jej otrzymania. Uwagi przekazywane będą pocztą elektroniczną (e-mail). Wykonawca zobowiązany jest uwzględnić uwagi Zamawiającego i przekazać dokumentację do ponownej akceptacji Zamawiającego, w terminie do 3 dni roboczych od otrzymania uwag.
- 5) Wykonawca, w terminie 10 dni roboczych od daty podpisania umowy, udostępni na własnej infrastrukturze sprzętowo-programowej, odpowiednią platformę e-learningową wraz ze szkoleniem z zakresu uzgodnionego z Zamawiającym. Udostępniona platforma wraz ze szkoleniem umożliwi przeprowadzenie szkoleń dla maksymalnie 2800 użytkowników Zamawiającego.
- 6) Po umieszczeniu przez Wykonawcę szkolenia na platformie e-learningowej, Wykonawca umożliwi Zamawiającemu przetestowanie działania platformy. W terminie 5 dni roboczych od daty udostępnienia Zamawiającemu przez Wykonawcę platformy do testowania, Zamawiający zweryfikuje poprawność działania platformy oraz udostępnione szkolenie i zaakceptuje lub zgłosi uwagi. Uwagi przekazywane będą pocztą elektroniczną (e-mail).
- 7) Udostępnienie użytkownikom platformy e-learningowej wraz ze szkoleniem nastąpi po akceptacji przez Zamawiającego udostępnionej platformy e-learningowej wraz ze szkoleniem, o której mowa w pkt. 2 ppkt 6).
- 8) Wykonawca zapewni dostęp do platformy e-learningowej tylko dla pracowników Państwowej Inspekcji Pracy.

- 9) Wykonawca musi zapewnić właściwe oznakowanie, zgodnie z pkt 2 ppkt 33:
- a) programu szkolenia,
 - b) treści umieszczonych na platformie e-learningowej,
 - c) zaświadczeń ukończenia szkolenia,
 - d) protokołu szkolenia.
- 10) Platforma szkoleniowa, na której udostępnione będzie szkolenie powinna umożliwić dostęp maksymalnie 2800 użytkownikom jednocześnie. Czas realizacji szkolenia powinien wynosić minimalnie 4 godziny dydaktyczne (1 godzina dydaktyczna = 45 min), natomiast maksymalnie 6 godzin dydaktycznych. Uczestnicy mają dostęp do szkolenia przez cały czas trwania zamówienia, z możliwością realizacji w dowolnym czasie bez ograniczeń co do pory dnia i miejsca realizacji. Uczestnik realizuje szkolenie jednokrotnie, z zastrzeżeniem możliwości ponownego przystąpienia do testu końcowego w przypadku jego niezaliczenia.
- 11) Usługa dostępu do platformy e-learningowej świadczona będzie przez Wykonawcę od dnia podpisania umowy – z uwzględnieniem terminów pośrednich wskazanych w Opisie Przedmiotu Zamówienia - do 31 maja 2026 roku.
- 12) Wykonawca będzie prowadził dokumentację w postaci zestawień uczestników, którzy rozpoczęli i ukończyli szkolenie (imię, nazwisko, jednostka organizacyjna, data rozpoczęcia i zakończenia szkolenia) oraz rejestru wydanych zaświadczeń.
- 13) Wykonawca przedstawi Zamawiającemu protokół odbioru szkolenia, podsumowujący całość realizacji zamówienia, uwzględniający dane wszystkich uczestników, którzy przystąpili do realizacji szkolenia i przeszli przez testy końcowe. Protokół będzie zawierał: imię i nazwisko uczestnika, nazwę jednostki organizacyjnej oraz zbiorcze zestawienie wyników testów końcowych i zbiorcze wyniki ankiety wstępnej, umożliwiające Zamawiającemu orientacyjną ocenę przyrostu kompetencji uczestników szkolenia. Zamawiający zatwierdzi protokół lub zgłosi do niego uwagi.
- 14) Wykonawca w ramach usługi zapewni funkcjonalność przesyłania przypomnień o konieczności ukończenia szkolenia do pracowników, którzy rozpoczęli szkolenie. Treść przypomnienia zostanie uzgodniona z Zamawiającym i będzie przesyłana raz w tygodniu.

- 15) Wykonawca przygotowuje i przekazuje, w formie elektronicznej, wszystkim uczestnikom szkolenia, imienne zaświadczenia o ukończeniu szkolenia (zaświadczenie, którego wzór akceptuje Zamawiający powinno zawierać: temat, datę ukończenia, imię i nazwisko uczestnika szkolenia, logo Wykonawcy). Zamawiający dopuszcza możliwość samodzielnego wygenerowania i wydruku zaświadczenia przez uczestnika po ukończeniu szkolenia za pośrednictwem platformy e-learningowej.
- 16) Wykonawca prześle Zamawiającemu, w formie elektronicznej, nie później niż 14 dni przed zakończeniem okresu udostępnienia usługi, zestawienie osób, które ukończyły szkolenie (co najmniej: imię, nazwisko, jednostka organizacyjna).
- 17) W ramach zamówienia Wykonawca będzie administrował, zarządzał platformą e-learningową i utrzymywał jej bezawaryjne działanie.
- 18) Wymagania techniczne:
- a) Platforma szkoleniowa udostępniana w modelu usługi on-line (SaaS).
 - b) Wsparcie dla przeglądarek Google Chrome, Firefox i Microsoft Edge.
- 19) Funkcje administrowania platformą szkoleniową, w szczególności:
- a) Tworzenie, edytowanie i usuwanie kont użytkowników.
 - b) Dodawanie użytkowników do platformy z poziomu interfejsu (formularz).
 - c) Masowe dodawanie użytkowników do platformy poprzez import pliku .csv.
 - d) Tworzenie, edytowanie i usuwanie grup użytkowników.
- 20) Funkcje administrowania procesem szkolenia:
- a) Śledzenie postępów użytkowników w trakcie szkolenia.
 - b) Wyświetlanie listy aktywności każdego użytkownika wraz z informacją o dacie i rodzaju aktywności.
 - c) Podgląd wyniku postępu nauki użytkowników w danym materiale szkoleniowym (test).
 - d) Konfigurowanie parametrów testów, w tym progu zaliczenia.
 - e) Uzyskiwanie statystyk prowadzonego szkolenia.
 - f) Generowanie certyfikatów ukończenia szkolenia.
- 21) Platforma e-learningowa powinna umożliwiać zarządzanie treścią szkoleniową przygotowaną w ramach zamówienia.

- 22) Platforma e-learningowa wraz z infrastrukturą powinna umożliwiać w ramach przygotowanego szkolenia:
- a) wysoką szybkość działania (tj. bez zauważalnych opóźnień w ładowaniu stron),
optymalizację pod kątem przepustowości łącz, polskojęzyczny interfejs użytkownika o intuicyjnej obsłudze,
 - b) działanie, poprzez Internet, w systemach operacyjnych Windows i Linux, w przeglądarkach internetowych – bez konieczności instalacji dodatkowych komponentów – Microsoft Edge (w tym tryb zgodności), Mozilla Firefox oraz Google Chrome,
 - c) implementację i osiągnięcie pełni funkcjonalności w obsłudze szkolenia przygotowanego zgodnie ze standardami SCORM,
 - d) odtwarzanie narracji audio i innych ścieżek dźwiękowych w funkcjonalnym playerze, interakcje z materiałem, wyświetlanie grafik i animacji oraz zapewnienie interakcji z nimi,
 - e) dostępność funkcji druku materiałów dydaktycznych dla uczestników,
 - f) zapewnienie wysokiego stopnia zabezpieczenia danych, w tym danych osobowych,
 - g) Szkolenia będą prawidłowo funkcjonowały na urządzeniach mobilnych spełniających minimalne parametry:
 - (1) System operacyjny Android w najnowszej wersji na dzień podpisania Umowy oraz minimum dwie wersje wstecz,
 - (2) System operacyjny iOS w najnowszej wersji na dzień podpisania Umowy oraz minimum dwie wersje wstecz.
 - h) Platforma e-learningowa nie może wymagać od użytkowników instalowania dodatkowego oprogramowania ani korzystania ze sprzętu innego niż standardowo wykorzystywany przez Zamawiającego.
- 23) Adres strony logowania do platformy e-learningowej, na której udostępnione będzie szkolenie wraz z opisem sposobu zalogowania się do szkolenia, będzie dostępny (podlinkowany) w dedykowanym e-mailu, wygenerowanym przez Wykonawcę dla użytkownika.
- 24) W ramach realizacji szkolenia Wykonawca zapewni uczestnikom możliwość zgłaszania pytań i wątpliwości dotyczących treści szkolenia za pośrednictwem platformy e-learningowej lub drogą elektroniczną. Wykonawca opracuje zestaw najczęściej zadawanych pytań wraz z odpowiedziami (FAQ) odnoszących się do zagadnień poruszanych na szkoleniu. Zestaw FAQ zostanie udostępniony uczestnikom szkolenia oraz przekazany Zamawiającemu.

25) Wykonawca zapozna wszystkich Uczestników z klauzulą informacyjną o przetwarzaniu ich danych osobowych (spełniającą wymagania art. 13 RODO) oraz uzyska od nich zgody na przetwarzanie danych osobowych i przekaże je Zamawiającemu.

Wykonawca wprowadzi i będzie stosować odpowiednie regulacje dotyczące przetwarzania danych osobowych i ochrony tajemnicy prawnie chronionej, w szczególności:

- a) zapewni odpowiednią politykę ochrony danych osobowych użytkowników platformy e-learningowej,
- b) zapewni odpowiednią ochronę informacji dotyczących aktywności poszczególnych użytkowników na platformie e-learningowej, zawartości materiałów dydaktycznych, w tym treści generowanych przez użytkowników,
- c) zapewni szyfrowanie SSL we wszystkich przypadkach, gdy wysyłane są dane osobowe. Szyfrowanie SSL musi być widoczne w pasku adresu przeglądarki za pomocą przedrostka „https://”. Certyfikat wykorzystany do szyfrowania SSL musi być rozpoznawany jako zaufany w najnowszych wersjach przeglądarek zdefiniowanych do obsługi platformy e-learningowej,
- d) zapewni oprogramowanie antywirusowe na platformie e-learningowej, zabezpieczające stale treści szkoleniowe oraz zasoby publikowane przez użytkowników,
- e) podpisze z Zamawiającym Umowę powierzenia przetwarzania danych osobowych, zgodną z art. 28 RODO, na warunkach określonych we wzorze stanowiącym załącznik do umowy głównej,
- f) opracuje projekt DPIA (art. 35 RODO) i przekaże Zamawiającemu do akceptacji w terminie 5 dni roboczych od podpisania umowy,
- g) zapewni retencję danych zgodnie z art. 5 ust. 1 lit. e RODO oraz aktualnymi wytycznymi w zakresie kwalifikowalności wydatków KPO, zapewniając dostępność danych do celów kontrolnych przez wymagany okres archiwizacji dokumentacji projektu, oraz przekazując Zamawiającemu wymagane rejestry i zestawienia zgodnie z pkt 2 ppkt 12) i pkt 2 ppkt 16),
- h) umieści klauzulę informacyjną RODO (art. 13 RODO) na pierwszej stronie platformy e-learningowej oraz w wiadomości powitalnej kierowanej do Uczestników.

- 26) Wykonawca zapewni uczestnikom szkolenia wsparcie techniczne i merytoryczne podczas realizacji szkolenia w postaci wyznaczenia osoby do kontaktu ze strony Wykonawcy.
- 27) Uczestnicy szkolenia będą realizować szkolenie e-learningowe z wykorzystaniem sprzętu komputerowego oraz urządzeń mobilnych, którymi aktualnie dysponują, zarówno w miejscu pracy jak i poza nim. Zamawiający nie zapewnia uczestnikom dodatkowego sprzętu ani oprogramowania na potrzeby realizacji szkolenia. Wykonawca zobowiązany jest zapewnić, aby szkolenie nie wymagało instalacji dodatkowego oprogramowania oraz było kompatybilne z powszechnie stosowanymi systemami operacyjnymi i przeglądarkami internetowymi.
- 28) Uczestnicy szkolenia zostaną wskazani przez Zamawiającego. Uczestnikami będą pracownicy Państwowej Inspekcji Pracy korzystający w codziennej pracy z systemów teleinformatycznych, nieposiadający specjalistycznej wiedzy z tematu przedmiotu zamówienia. Szkolenie powinno być dostosowane do potrzeb pracowników nieposiadających specjalistycznej wiedzy informatycznej.
- 29) Wykonawca uwzględni w formularzu wyceny wszystkie koszty, jakie Państwowa Inspekcja Pracy Główny Inspektorat Pracy będzie zobowiązany ponieść w związku z realizacją szkolenia.
- 30) Zamawiający oświadcza, że szkolenie jest bezpośrednio związane z wykonywaną pracą zawodową uczestników, w tym z obowiązkami służbowymi wynikającymi z zatrudnienia w Państwowej Inspekcji Pracy i ma na celu podnoszenie lub aktualizację kwalifikacji zawodowych pracowników i będzie całkowicie finansowany ze środków publicznych.
- 31) Wykonawca oświadcza, że świadczone przez niego szkolenie stanowi usługę kształcenia zawodowego lub przekwalifikowania zawodowego, o której mowa w art. 43 ust. 1 pkt 29 ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług, oraz że spełnione są przesłanki do zastosowania zwolnienia z podatku VAT.
- 32) Wykonawca jest zobowiązany do używania w komunikacji z uczestnikami języka, który będzie:
- a) przeciwdziałający stereotypowemu postrzeganiu ról kobiet i mężczyzn,
 - b) zgodny z zasadami niedyskryminacji, szczególnie ze względu na niepełnosprawność.
- 33) Wykonawca zobowiązuje się umieszczać, na wszelkich materiałach wytworzonych w ramach realizacji zamówienia związanych z organizacją szkoleń, aktualnie obowiązujące logotypy oraz informację

o współfinansowaniu projektu: „Zamówienie dofinansowane ze środków Unii Europejskiej, Krajowego Planu Odbudowy i Zwiększania Odporności finansowanego ze środków Instrumentu na Rzecz Odbudowy i Zwiększania Odporności; Inwestycja: C3.1.1. Cyberbezpieczeństwo - CyberPL , infrastruktura przetwarzania danych oraz optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo; Cyberbezpieczeństwo - Cyberbezpieczny Rząd – w ramach projektu pn. „Cyberbezpieczeństwo w PIP”, na podstawie porozumienia o powierzenie grantu o numerze KPOD.05.10- CR.01-001/24/0036/ KPOD.05.10-CR.01-001/25/2025.” Wykonawca jest zobowiązany do zapoznania się z oficjalnymi dokumentami w ramach Krajowego Planu Odbudowy i Zwiększania Odporności oraz ich aktualizacjami, a nade wszystko ze Strategią Promocji i Informacji KPO oraz Księgą Identyfikacji Wizualnej KPO. Dokumenty są dostępne pod adresem: <https://www.gov.pl/web/aktywa-panstwowe/krajowy-plan-odbudowy-i-zwiekszania-odpornosci>